

Getronics Government Solutions

Bridge Certification Authority Demonstration Phase II

Software Development and Support

2 August 2001

John.Pawling@GetronicsGov.com

Getronics BCA II Support

- **Supported Getronics-developed freeware:**
 - **Access Control Library (ACL)**
 - **S/MIME Freeware Library (SFL)**
 - **Certificate Management Library (CML)**
 - **Enhanced SNACC ASN.1 software**
 - **Crypto Token Interface Libraries (CTIL)**
- **Enhanced ACL to meet BCA II requirements for processing X.509 Attribute Certificates.**
- **Provided facilities support, installation, integration, testing and hosting of BCA demos.**

Getronics Security Services Objectives

- **Provide freeware reference implementations of:**
 - **X.509 v3 certification path building and verification**
 - **Rule Based Access Control**
 - **IETF S/MIME v3 security protocol**
 - **Abstract Syntax Notation.1 (ASN.1) encoding and decoding (Distinguished Encoding Rules (DER))**
- **Provide unencumbered source code for libraries**
- **Provide modular, high-level, portable interface:**
 - **Minimizes effort required by application developers to meet security requirements**
 - **Allows developers to use only the libraries required for their particular application**

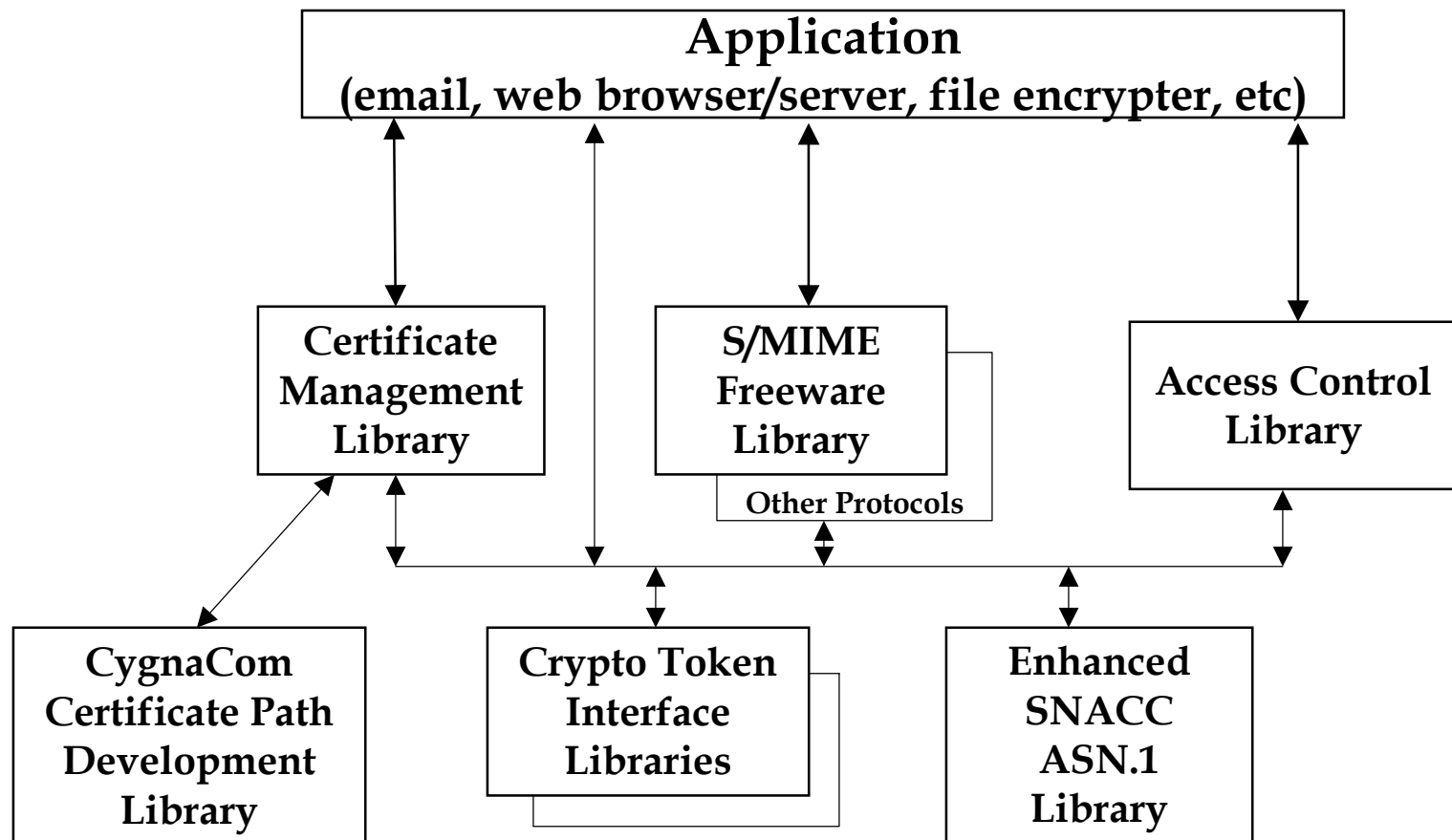
Getronics Security Services Libraries

- **Certificate Management Library**
 - Builds and validates X.509 certification paths & CRLs
 - Provides local cert/CRL storage functions
 - Provides remote directory retrieval via LDAP
- **S/MIME Freeware Library**
 - Implements IETF S/MIME v3 security protocol
 - Security label, signed receipts, mail list support
- **Access Control Library**
 - Provides Rule Based Access Control using security labels & authorizations as per SDN.801
 - Implements Attribute and X.509 Certificates
 - Meets DMS and Bridge CA Phase II Requirements
- **Enhanced SNACC ASN.1 software provides DER.**

Getronics Freeware Availability

- **S/MIME Freeware Library**
<http://www.getronicsgov.com/hot/sfl_home.htm>
- **Certificate Management Library**
<http://www.getronicsgov.com/hot/cml_home.htm>
- **Access Control Library**
<http://www.getronicsgov.com/hot/acl_home.htm>
- **Enhanced SNACC – ASN.1 Toolkit supports DER.**
<http://www.getronicsgov.com/hot/snacc_home.htm>
- **For all Getronics freeware libraries, unencumbered source code is freely available to all. Getronics freeware can be used without paying any royalties or licensing fees. There is a public license associated with each freeware library.**

Getronics Security Services Architecture



S/MIME Freeware Library

- **SFL is a freeware implementation of IETF S/MIME v3 RFC 2630 (Cryptographic Message Syntax) & RFC 2634 (Enhanced Security Services) specs.**
- **When used with Crypto++ freeware library, SFL implements RFC 2631 Diffie-Hellman Key Agreement Method (Ephemeral Static).**
- **SFL supports the use of RFC 2632 (Certificate Handling) and RFC 2633 (Message Specification).**
- **Goal: To provide a reference implementation of RFC 2630 and RFC 2634 to encourage their acceptance as Internet Standards.**

S/MIME Freeware Library

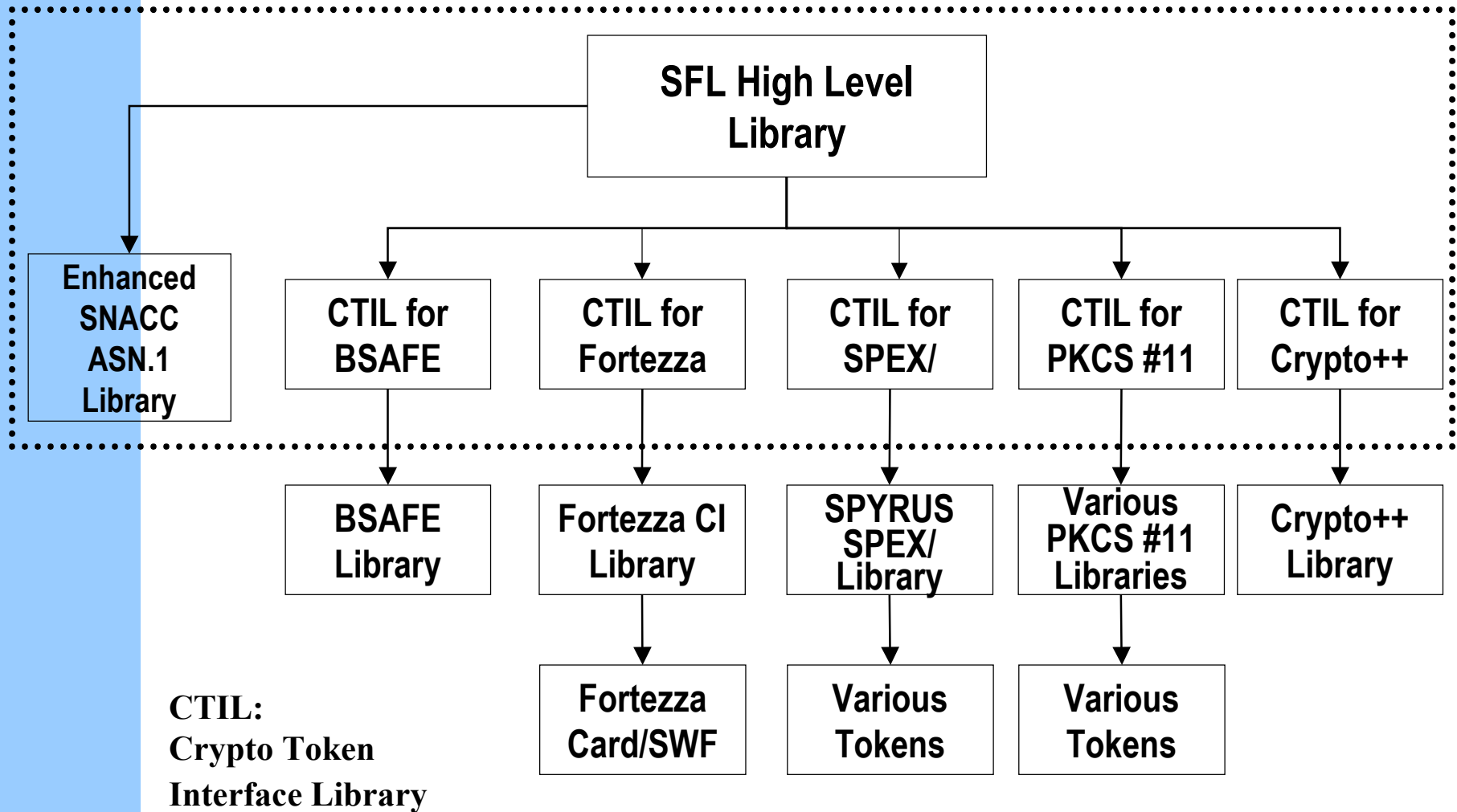
- **Protects any type of data (not just MIME).**
- **Algorithm independent: SFL is used with external crypto libraries that provide a variety of crypto algorithms.**
- **Uses Getronics-enhanced SNACC freeware library to perform all ASN.1 encoding (including DER) and decoding of CMS and ESS objects as well as certificates, Certificate Revocation Lists, etc.**
- **SFL does not build/process MIME headings.**

S/MIME Freeware Library

Implements optional RFC 2634 security services:

- **Signed receipts – provides authenticated proof of delivery (similar to registered mail).**
- **Security labels – provides the capability to label data with sensitivity values (e.g.; company proprietary; private medical information; etc).**
- **Mail list information – supports the secure distribution of messages by mail list servers.**
- **Signing Certificate attribute - identifies signer's certificate(s), ACs and certificate policies.**

SFL Architecture



SFL Components

- **SFL High Level library**
 - Builds and processes CMS and ESS objects independent of the crypto library in use
 - Provides full C++ API and limited C API
- **Enhanced SNACC ASN.1 library**
 - Implements ASN.1 Distinguished Encoding Rules
- **Crypto Token Interface Libraries (CTIL)**
 - Isolates the SFL High Level classes from the specifics of the cryptographic token processing
 - Calls the cryptographic token functions to perform the Encrypt, Decrypt, Sign, Verify operations

Crypto Token Interface Libraries

- **BSAFE CTIL:** Calls RSA BSAFE library providing RSA algorithms such as RSA, RC2, MD5.
- **Crypto++ CTIL:** Calls Crypto++ library providing 3DES, E-S D-H, SHA-1, DSA, RSA, etc.
- **Fortezza CTIL:** Calls Fortezza Cryptologic Interface library using Fortezza Card/Software Fortezza providing SKIPJACK, Key Exchange Algorithm, SHA-1 and DSA.
- **SPEX/ CTIL:** Calls SPYRUS SPEX/ library providing access to a variety of crypto tokens/algorithms.
- **PKCS #11 CTIL:** Provides access to PKCS #11-compliant crypto libraries. Tested with Litronic Maestro, GemPlus and DataKey PKCS #11 libraries.

SFL Interoperability Testing

- **SFL S/MIME v2 interop testing: SFL used to exchange signedData and envelopedData messages with Microsoft Internet Explorer Outlook Express v4.01, Netscape Communicator 4.X, Entrust and Baltimore MailSecure S/MIME v2 products.**
- **SFL S/MIME v3 interop testing (see later slides): Tested the majority of features in RFCs 2630 (CMS), 2631 (D-H) and 2634 (ESS) as well as some of the features in RFC 2632 (Cert) and 2633 (Msg). SFL does not support every S/MIME v3 optional feature and does not build/process MIME headers.**

SFL Interop Testing (cont'd)

- **Used SFL to successfully process and produce sample data in "Examples of S/MIME Messages". Complete test drivers and test data provided as part of SFL release. SFL-generated data in Examples-06 such as: signed receipts, countersignatures, security labels, equivalent labels, mail list info, signing certificate attribute.**
- **S/MIME v3 interop testing between SFL & Microsoft successfully tested almost all signedData & envelopedData features. Included DSA, 3DES, E-S D-H, RSA and Fortezza algorithms. For example, SFL (using Crypto++) exchanged E-S D-H-protected envelopedData. Almost all ESS features tested (signed receipts).**

SFL Status

- **Version 1.10 SFL released in April 2001**
 - **Implements RFC 2630 (CMS) & RFC 2634 (ESS)**
 - **Tested on MS Windows NT/98/2000, RedHat Linux & Sun Solaris 2.7.**
- **Future versions will include:**
 - **Further testing of PKCS #11 CTIL**
 - **Implementing changes to IETF specs**
 - **Support for other operating systems**
 - **Add "Certificate Management Messages over CMS" ASN.1 encode/decode functions**

Certificate Management Library

- Builds and validates X.509 certification paths & CRLs as specified in 2000 X.509 Recommendation.
- Performs ASN.1 decoding of Certificates, CRLs, and components thereof.
- Supports both X.509 v3 certs & Fortezza v1 certs
- Uses CTILs to support variety of crypto algorithms (such as verifying DSA & RSA signatures).
- Uses CygnaCom Certificate Path Development Library (CPDL) to robustly build cert paths
- Meets all Bridge Certification Authority (BCA) Phase II requirements (such as using cross certs.)

Certificate Management Library

- **Accompanying Storage and Retrieval Library (SRL) (optionally) provides local certificate and CRL storage management functions.**
- **SRL (optionally) provides remote directory retrieval capabilities using Lightweight Directory Access Protocol (LDAP).**
- **CML was originally developed by U.S. Government.**
- **CML provides a C language API.**

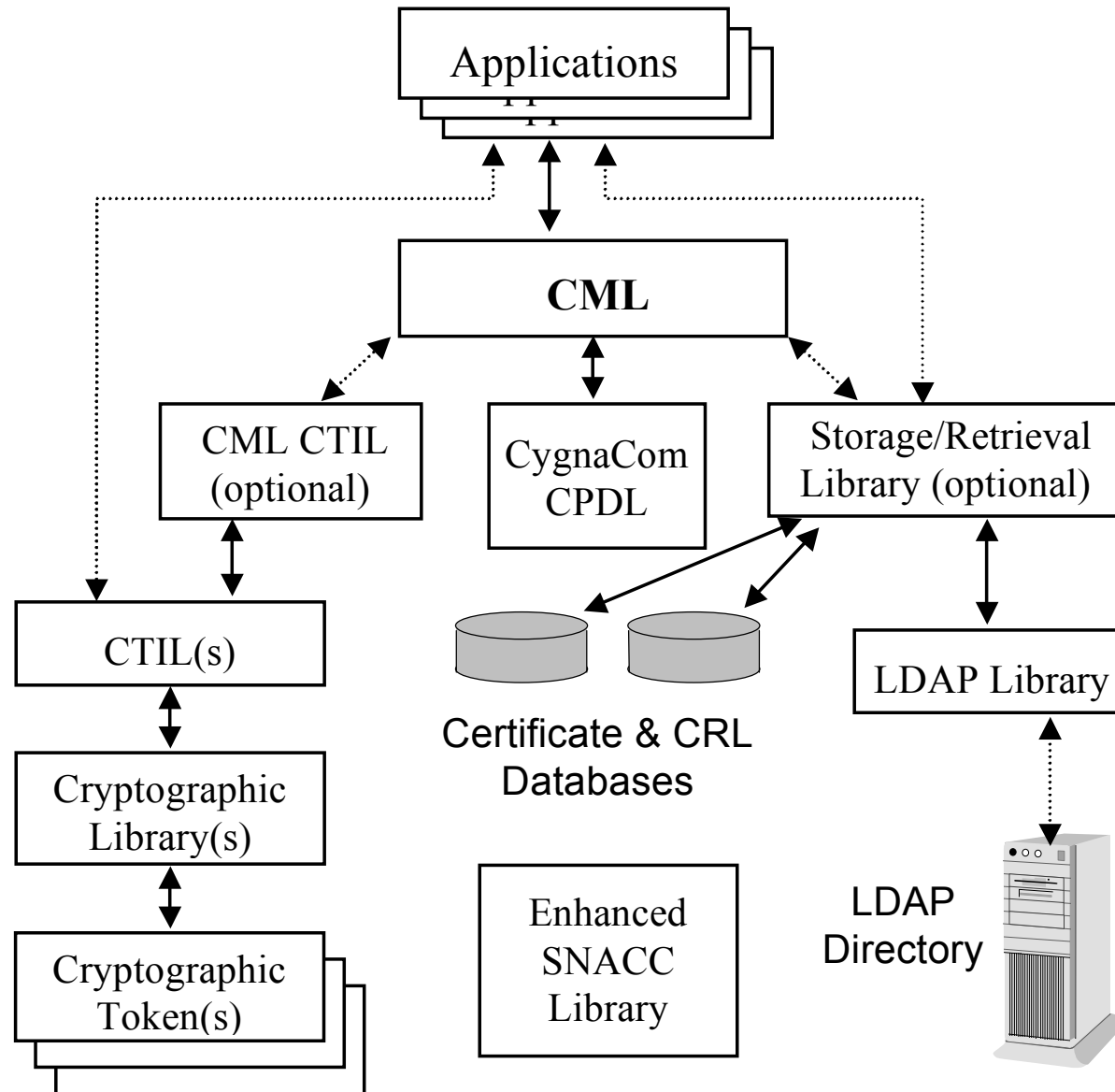
CML X.509 Compliance

- **Implements majority of 2000 X.509 features and cert path validation requirements:**
 - name chaining (including multi-valued RDNs)
 - key identifier chaining
 - signature verification (using DSA and RSA)
 - validity date checking
 - revocation checking
 - name constraints
 - basic constraints
 - certificate policies, mappings and constraints
 - subject and issuer alternate names
 - key usage/extended key usage
 - private key usage period
 - CRL distribution points
 - cross certificates
 - CRL extensions and CRL entry extensions

CML PKIX Compliance

- **CML complies with majority of IETF PKIX requirements in RFC 2459. PKIX requirements CML doesn't support include: Delta CRLs. The CML will continue to be enhanced to maximize PKIX compliance.**

CML Architecture



CML Interop Testing

- **CML has been thoroughly tested including interoperability testing with a variety of Certification Authority (CA) products.**
- **For example, CML has been used to verify certification paths created by VeriSign, Entrust, Microsoft, Motorola, General Dynamics, Baltimore, Netscape and SpyruS CA products.**
- **As part of BCA Demo Phase II testing, CML successfully verified certification paths including certificates created by multiple vendors and cross certificates.**

CML Interop Testing

- **National Institute of Standards and Technology (NIST) provides a standard test suite of X.509 certificate paths at:
<<http://csrc.nist.gov/pki/testing/x509paths.html>>**
- **This data can be used for testing applications for compliance with RFC 2459 PKIX Certificate and CRL Profile.**
- **CML was used to successfully process NIST test data.**

CML Status

- **Version 1.9.2 CML released in July 2001**
 - **Fixes bugs in earlier releases.**
 - **Tested on MS Windows NT/98/2000, RedHat Linux & Sun Solaris 2.7.**
- **Future versions will include:**
 - **Support for Delta CRLs and these 2000 X.509 extensions: CRL scope, CRL stream identifier, Delta information, Freshest CRL, Ordered list, and Status referral.**
 - **Implement changes to X.509 and IETF specs.**
 - **Expand CML API to include C++ API based on SNACC C++ classes, but preserve C API for backwards-compatibility and for C developers.**

Access Control Library

- **ACL provides Access Control Decision Function supporting SDN.801 Partition Rule Based Access Control requirements using: Clearance attribute containing subject's authorizations; security label indicating sensitivity of data; and Security Policy Information File (SPIF).**
- **ACL uses SPIF as part of process of ensuring that subject's authorizations are commensurate with values in security label.**
- **By using SPIFs, ACL can support a variety of security policies and equivalency mappings between security policy values.**

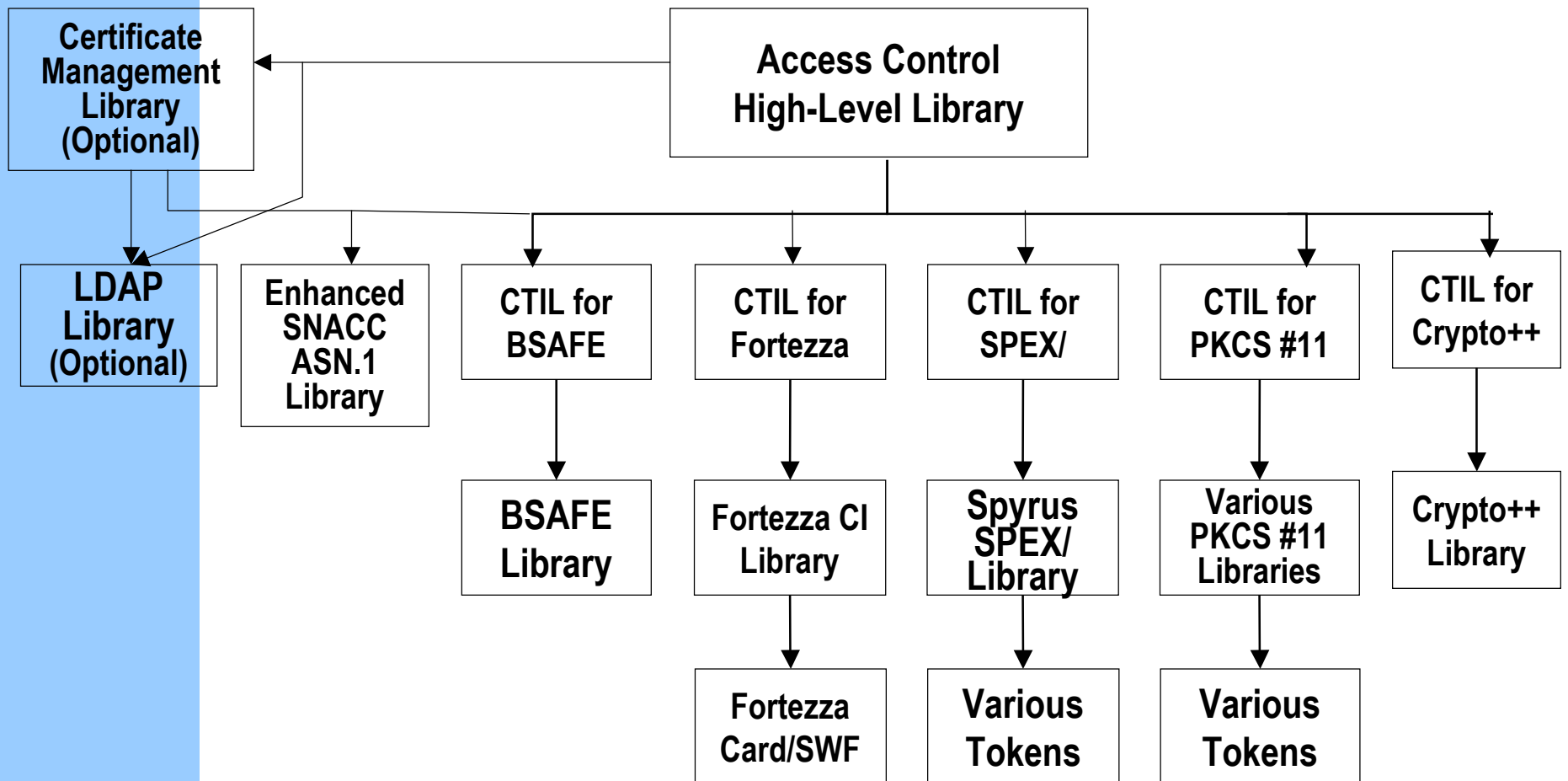
Access Control Library

- **ACL checks a security label to ensure it includes a valid combination of security classification and security category values (see SDN.801) as specified in SPIF for security policy identified in label.**
- **ACL verifies Attribute Certificates (AC) to meet BCA Demo Phase II requirements.**
- **ACL supports X.509 Certificates to meet DMS and Canadian MMHS requirements.**
- **Provides displayable string representation of a security label.**

Access Control Library

- **Optionally uses CML to build and verify v3 X.509 certification paths.**
- **Optionally uses Lightweight Directory Access Protocol to retrieve security objects.**
- **ACL provides a high-level C++ language API.**
- **ACL can be used with CTILs to support a variety of crypto algorithms (such as verifying DSA and RSA signatures).**
- **CygnaCom used ACL in their e-mail security plugin, Attribute Authority, trusted web server.**

ACL Architecture



ACL Status

- **Version 1.6 ACL released in May 2001**
 - **Supports multiple Clearance attributes in an X.509 Attribute or public key certificate to meet Canadian MMHS requirements.**
 - **Tested on MS Windows NT/98/2000.**
- **Future versions will include:**
 - **Support for other operating systems such as Linux and Solaris**
 - **Develop sophisticated test application.**
 - **May support additional requirements such as 2000 X.509 Recommendation, IETF PKIX AC, and alternative access control models.**

BCA CML/SFL/ACL Success

- **BCA demo is testing cross-certified Entrust, Motorola, Baltimore & SPYRUS PKIs. CML/CPDL successfully used to build and verify cross-certified certification paths between these PKIs.**
- **CygnaCom integrated SFL/CML/ACL/CPDL into a plug-in for Eudora Pro. Interop testing successful between SFL/CML/ACL/CPDL/Eudora client, Baltimore Mail Secure and Entrust S/MIME toolkit.**
- **CygnaCom used ACL in Attribute Authority.**
- **CygnaCom used ACL & CML in trusted web server.**
- **Raytheon integrated SFL/CML/CPDL into plug-in for Novell Groupwise e-mail application.**

BCA Interop Test Suite

- **We plan to develop a standard set of tests that will verify that an application meets BCA interop reqts:**
 - **developing certificate paths;**
 - **verifying certificate paths; and**
 - **implementing S/MIME in an interoperable way**
- **We will develop a document to specify the "BCA Interoperability Test Procedures" including positive and negative test cases.**
- **We will provide "canned" messages & certification path test data that a vendor can use to test their product (similar to PKI test data that we generated for NIST).**

BCA Interop Test Suite (cont'd)

- **We will configure an LDAP-accessible directory at Getronics to simulate the current BCA demo directory information tree.**
- **Applications will be able to use LDAP to directly access the directory to test their ability to retrieve the certificates and CRLs required to build complex certification paths composed of certificates from multiple PKIs.**
- **We will maintain BCA-compliant Entrust, Baltimore & CygnaCom e-mail clients installed in our lab.**
- **We will use those clients to send and receive test messages using each tester's unique key material.**

BCA Interop Test Suite (cont'd)

- **We will assist the vendors with executing the tests and providing troubleshooting hints.**
- **Our initial goal is to support testing of S/MIME applications, but we will design test suite to serve as a general certificate path development and processing test suite.**

NIST S/MIME v3 Test Facility

- **Getronics is developing open source S/MIME v3 auto responder using SFL, CML, Enhanced SNACC, CTILs.**
- **NIST plans to host auto responder on NIST web site.**
- **Vendors can use this facility to determine if products comply with S/MIME v3 specs & NIST profile.**
- **Auto responder processes S/MIME messages sent by tester & provides feedback regarding success/failure.**
- **Auto responder creates signed and/or encrypted S/MIME messages for processing by tester.**
- **Auto responder generates test key pairs & cert paths for each tester. It can use certs provided by tester.**

Point of Contact

John Pawling

John.Pawling@GetronicsGov.com

Getronics Government Solutions, LLC

141 National Business Pkwy, Suite 210

Annapolis Junction, MD 20701

(301) 939-2739 or (410) 880-6095